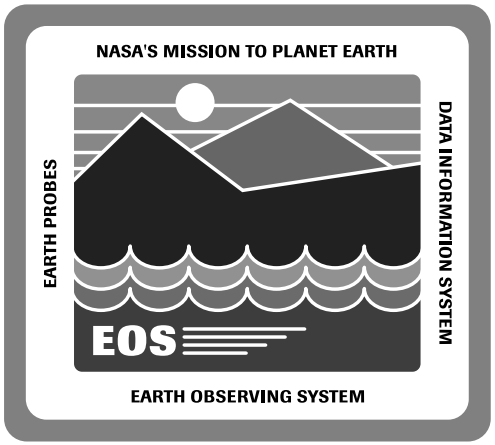


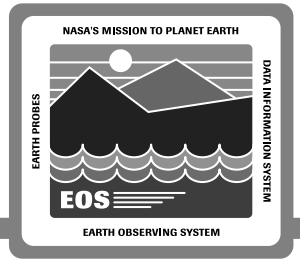
MSS - Accountability and Security Management

Yanamandra Sastry

ysastry@eos.hitc.com

ECS Release A SDPS/CSMS Critical Design Review
17 August 1995

Accountability Management Overview



Accountability Management provides the capability to generate audit trails, and maintain end-to-end accountability.

It has two implementations with different scopes:

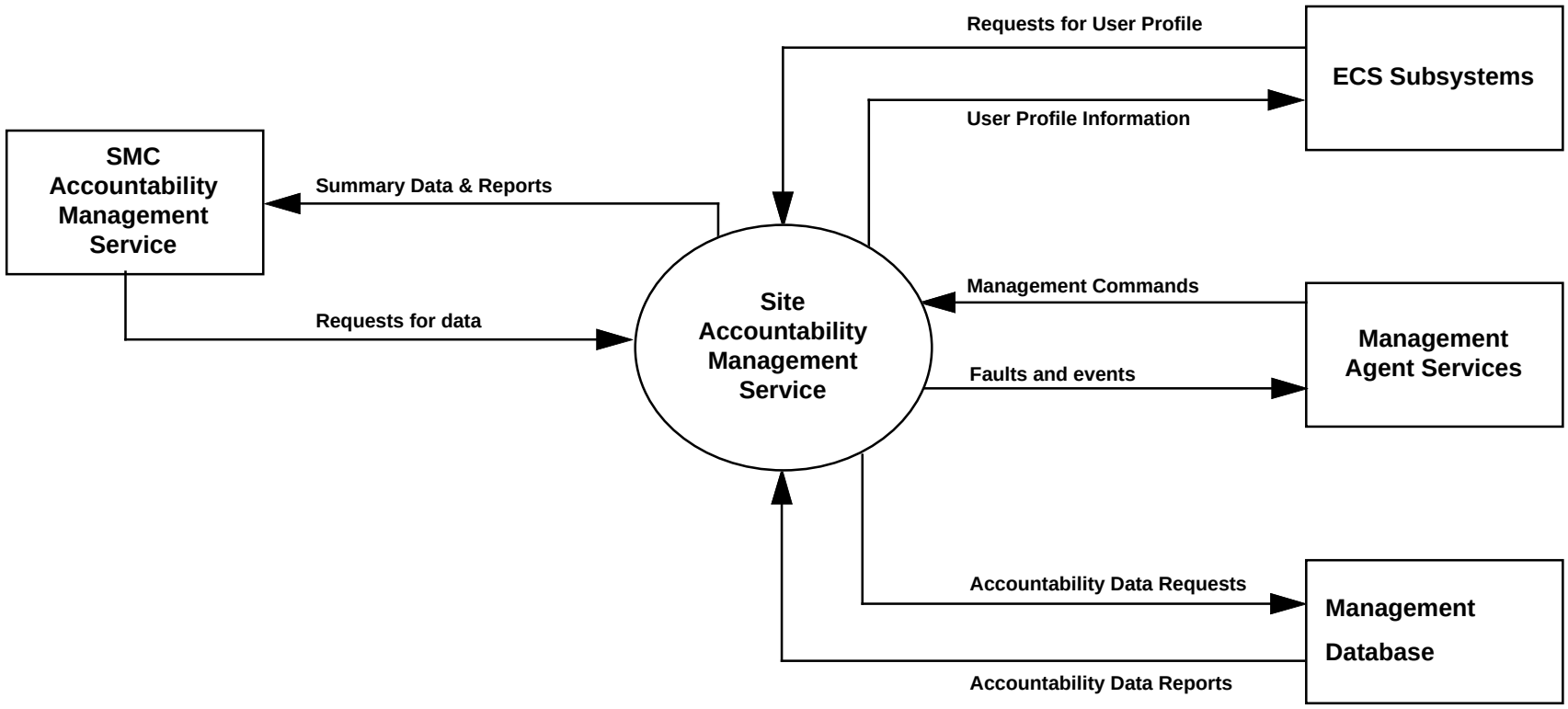
- **LSM - Site-Resource (data & services) level Accountability**
  - **Maintains detailed information on activities at the site**
  - **Monitors resource utilization at a site**
  - **Provides User Account Management**
- **SMC - System-wide Service level Accountability**
  - **Maintains summary data rolled up from the sites**
  - **Analyses this data for system-wide trends analysis/views**

Management and Presentation of Accountability Data

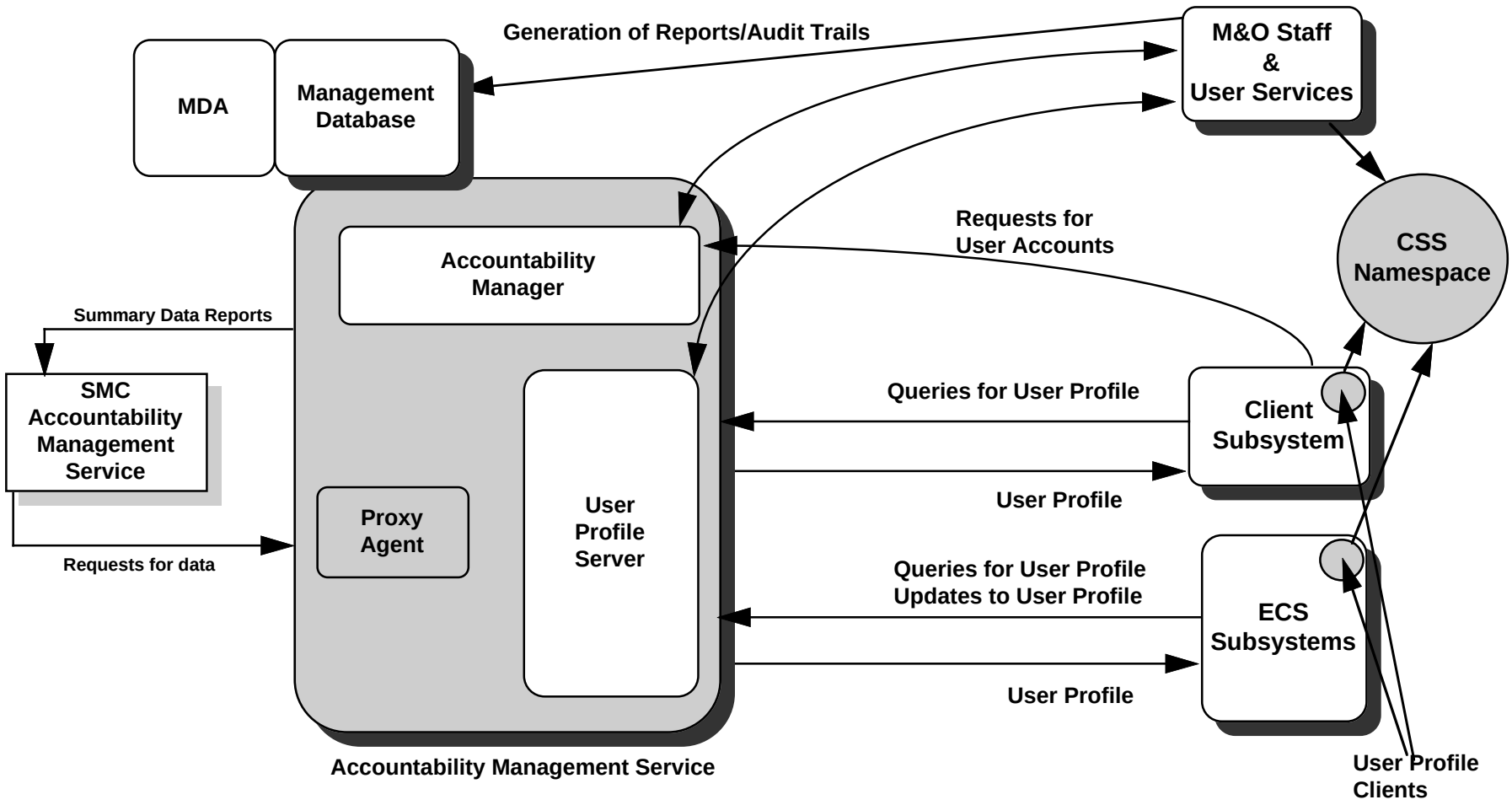
- **Provides the capability to generate standard and ad-hoc reports for performance, fault, security and activity analyses**

The service is largely custom-development

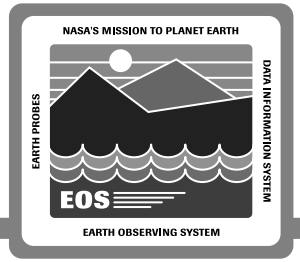
Accountability Management Context



Accountability Management Design

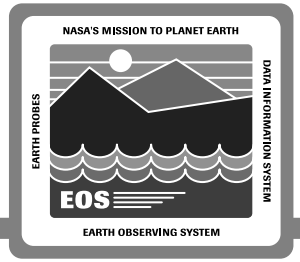


Design Description



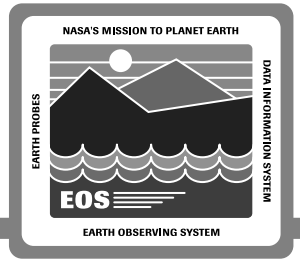
- **Components**
  - **Accountability Manager**
    - **Provides HTML GUI for User Account Creation/Management**
    - **Custom**
  - **User Profile Server**
    - **Provides dynamic parts of the User Profile**
    - **Custom**
  - **User Profile Client**
    - **Interface class used by other subsystems**
    - **Provides the User Profile to other subsystems**
    - **Custom**
  - **Management Proxy Agent**
    - **Reuse of ECS Custom Software**

Design Description (cont.)



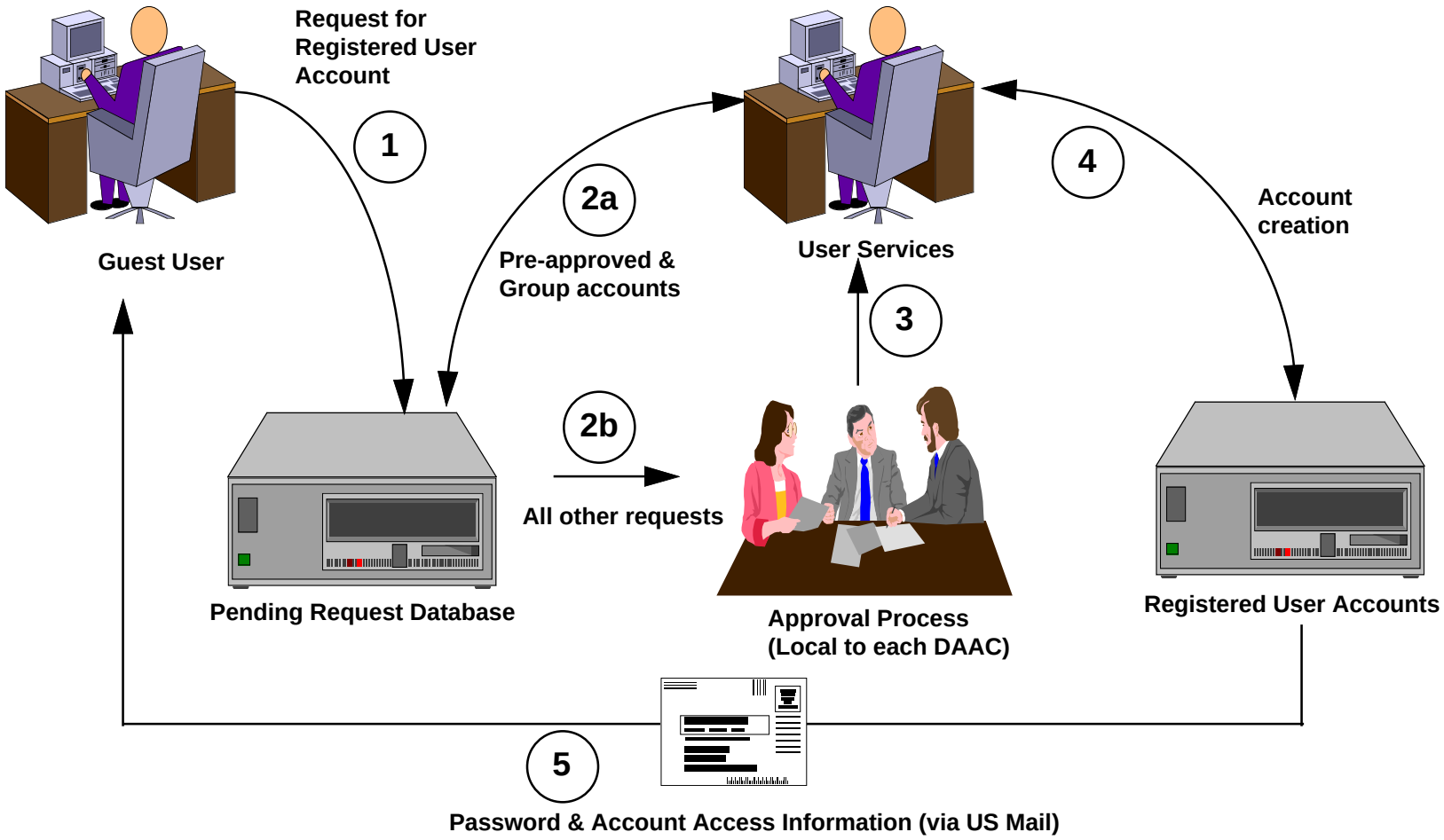
- **Interfaces**
  - **ECS Subsystems request User Profile**
  - **Management Data Access**
  - **Management Database**
  - **Management Proxy Agent**
    - **Provides for the management of the service**

User Account Information Management

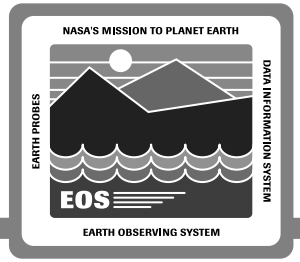


- HTML-based Graphical User Interface - Custom GUI
  - Conformant to ECS project-wide GUI design guidelines
  - Provides capability to create/maintain user accounts
  - Being Prototyped in EP6
- User profile made available through controlled access to User Services and other Subsystems on request.
- Used by Subsystems as in the following examples:
  - By the Science Data Server for the Electronic Mail Address of a user to send a notification to the user on the completion of a data acquisition request
  - By the Distribution Data Server for the Shipping Address used to print a mailing label for a request being shipped on media
  - By the Science Data Server for the Telephone Number of a user for an operator to contact the user
- Updated by users (via the Client subsystem)

Scenario - User Account Creation



Management and Presentation of Accountability Data



Accountability data comprises fault, performance, security and user activity data

This data is collected based on ECS events

Events may be low level events or system-level transactions (e.g., searches, browses, data acquisition requests)

Events are logged by the Agent to MSS History log files (one per host)

These log files are periodically consolidated & processed by MDA

The processed information is then loaded to the Management Database

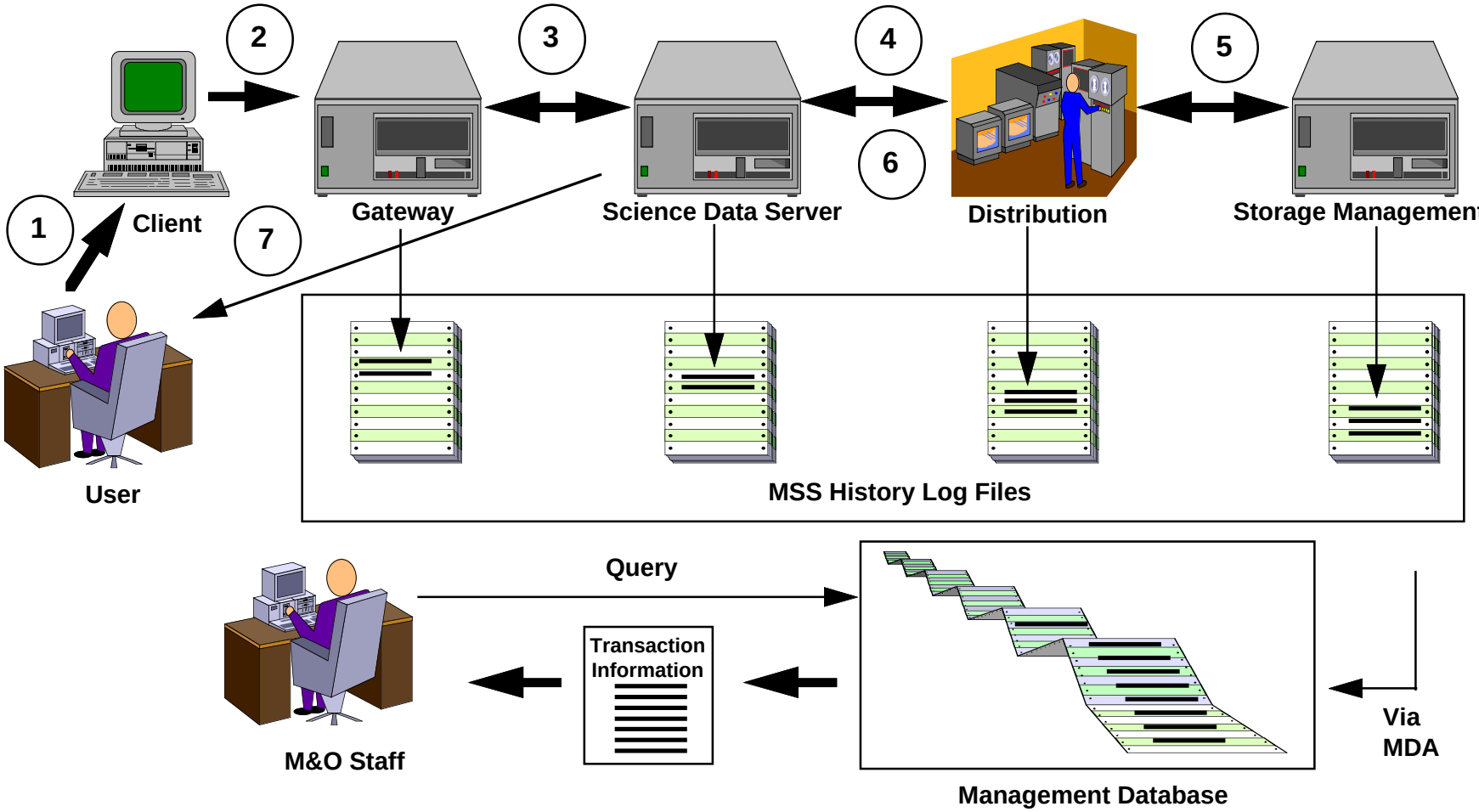
Analysis and Report Generation is done via Management Database tools

Standard reports generated are based on activity, such as:

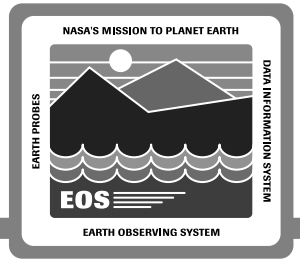
- **Number of data acquisition requests by user**
- **Number of data acquisition requests by data type**

The Management Database supports ad-hoc querying for additional report types

Scenario - User Data Acquisition

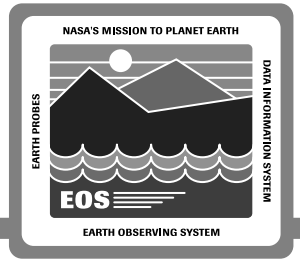


Scenario - Description



1) A user identifies data and the transmission mechanism
2) The Client subsystem transmits the transaction to the Gateway at the DAAC whose Data Server has the data product
3) The Gateway transmits the transaction to the Science Data Server
4) The Science Data Server queues the request to the Distribution Data Server
5) The Distribution Data Server dequeues the request, and using the services of Storage Management copies the data to disk or to media (based on the user's media preferences)
6) The Distribution Data Server sends a notification of the completion to the Science Data Server
7) The Science Data Server sends a notification to the user of the completion of the transaction

Scenario - Description (cont.)



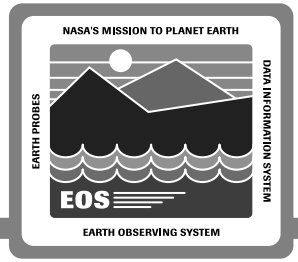
Events generated as a result of the steps in this scenario are logged to the MSS History Log files on the local host of each server in the transaction.

These History Log files are then consolidated at the MSS server by MDA, processed and loaded into the Management Database.

The Management Database may be queried in order to retrieve information on the data distributed (for a specified user and a time interval).

Start and stop events for each step allows the duration to be calculated for performance analysis, thereby allowing bottlenecks to be identified in system-level transactions.

Scenario - Description (cont.)



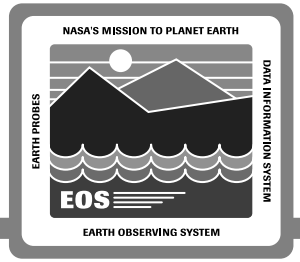
End-to-end transaction performance:

• The Client subsystem generates a unique identifier for the transaction which is passed to the Science Data Server. This identifies the start of the transaction.

• The Science Data Server (and every service downstream) generates a unique identifier which it passes to the downstream service, and logs its events with its identifier and the one received from the upstream service.

• This pair of identifiers facilitates the identification of all the subtransactions of an end-to-end transaction.

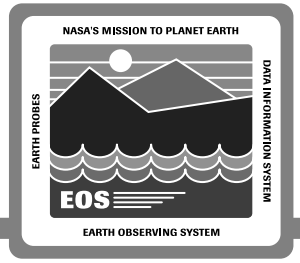
Summary



Largely custom-developed service:

- **Graphical user interface based on HTML**
- **User Profile server based on OODCE**
- **Handles events to system-level transactions**
- **Prototyping underway for EP**
- **Demonstration of User Account Management in the lab after the presentation**

Security Management Overview

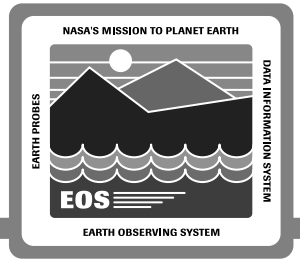


Security Management provides the following functional capabilities:

- **Security Database Management**
  - **Authentication**
    - **DCE-based authentication for internal users**
    - **Kerberos Authentication for external users**
  - **Authorization**
    - **Access to ECS network services based on source address**
    - **DCE-based authorization**
- **Compliance Management**
  - **Compliance to policies (e.g., passwords, file system integrity)**
- **Intrusion Detection**
  - **Unauthorized access to ECS resources and services**

Highly COTS-intensive - COTS products covered in next section

Security Management Overview (cont.)



Two implementations with different scope:

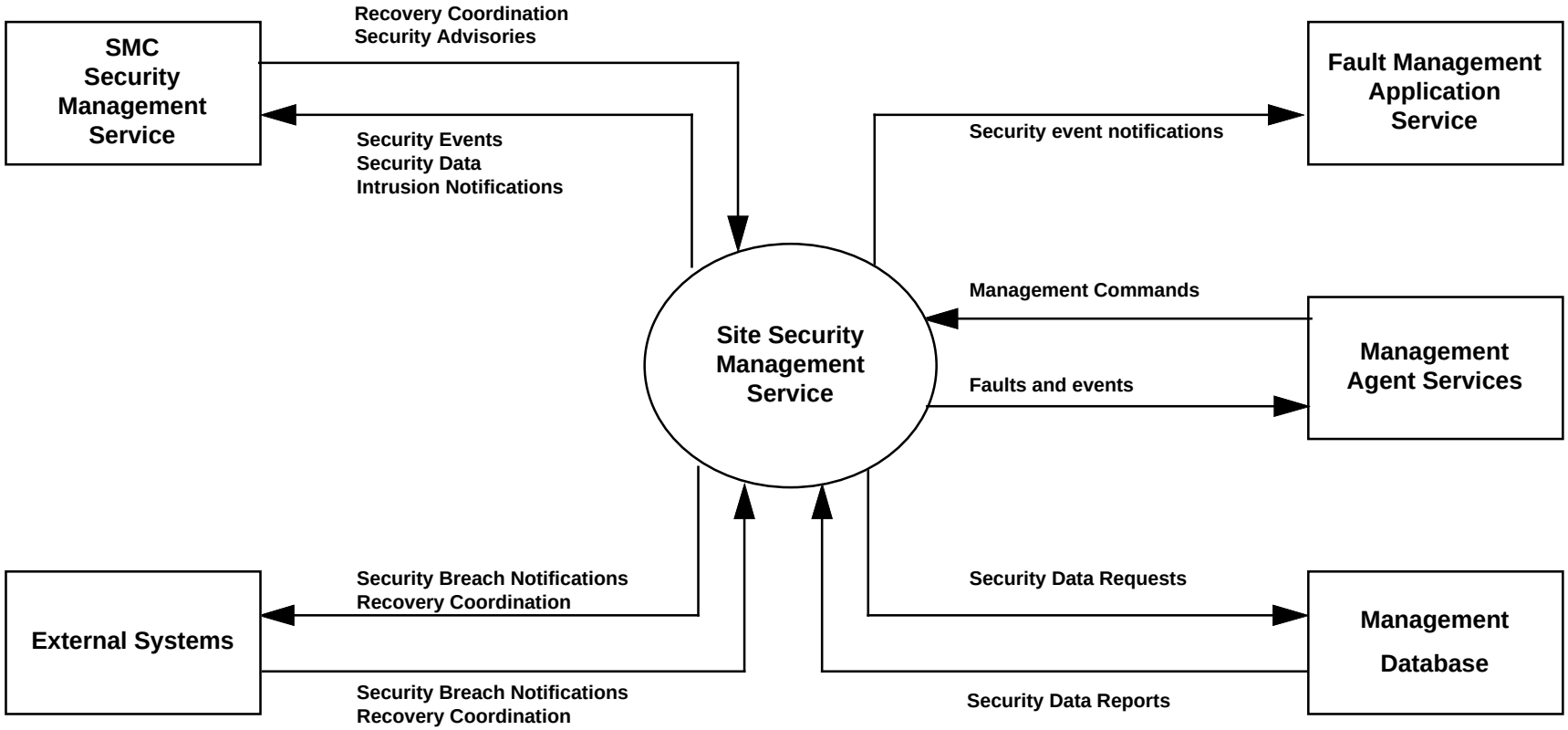
LSM

- **Manages site security**
- **Manages compliance to established policy**

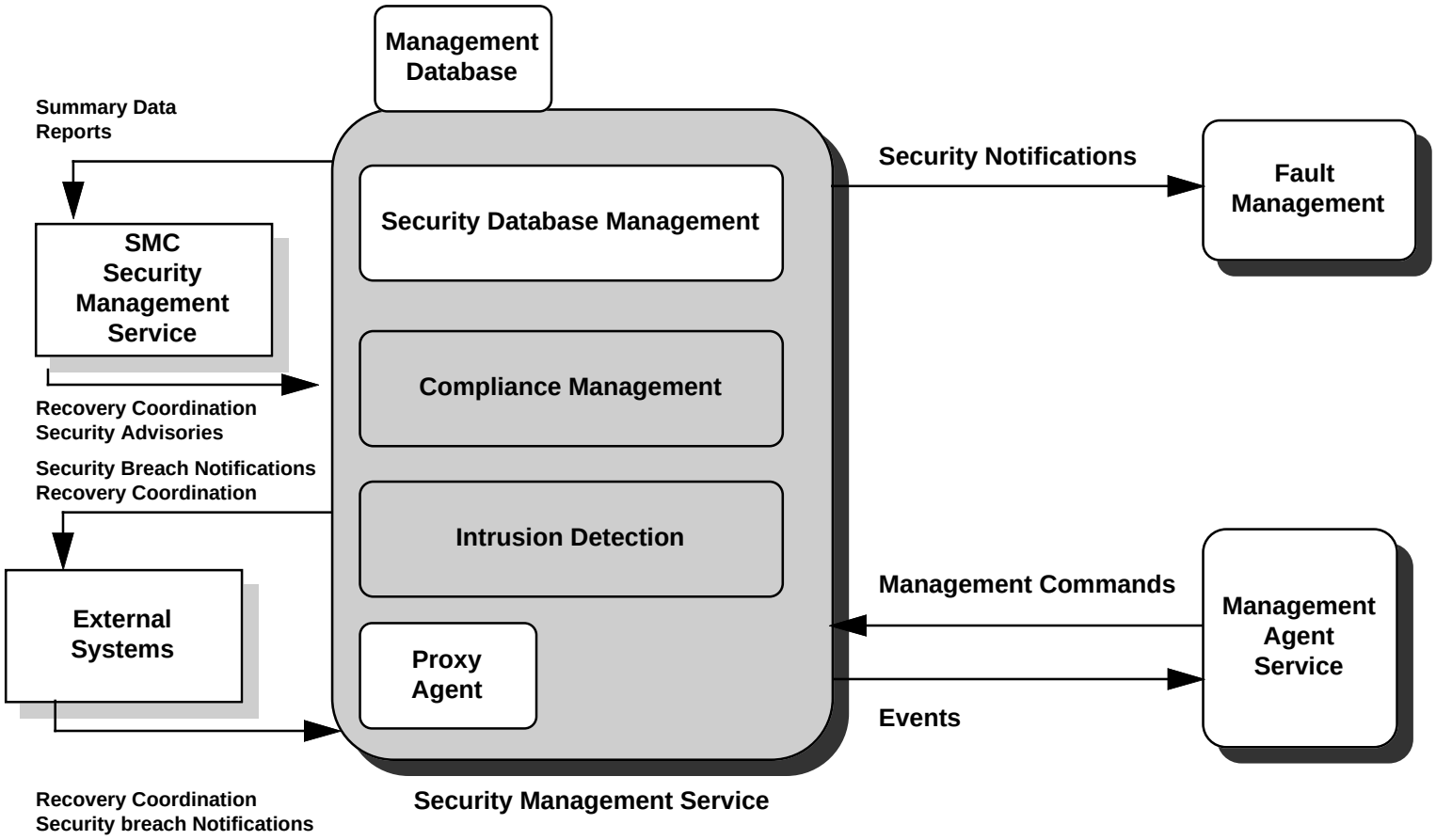
SMC

- **Monitors system-wide security**
- **Disseminates security policy**
- **Interfaces with external agencies such as CERT and NASIRC**

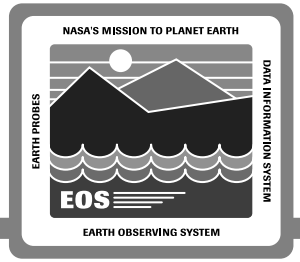
Security Management Context



Security Management Design



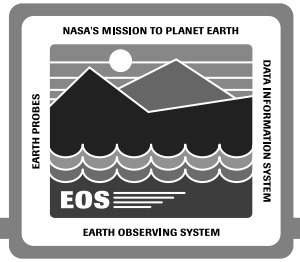
Design Description



Components:

- **Security Database Management:**
  - **HAL DCE Cell Manager**
    - **Management of DCE Security Registry, Namespace & Cell Configuration**
    - **COTS**
  - **Kerberos**
    - **Trusted third party network authentication**
    - **OTS**
  - **Router Configuration**
    - **Access control to ECS resources based on packet filtering based on source-destination pairs of ports/services**
    - **COTS + configuration**
  - **TCP Wrappers**
    - **Monitoring and control of access to network services on a host**
    - **OTS + Configuration**

Design Description (cont.)



- **Compliance Management:**
  - **COPS**
    - **Checks a host for vulnerabilities**
    - **OTS + Scripting**
  - **SATAN**
    - **Determination of the vulnerabilities of a host/network**
    - **OTS + Configuration**
  - **Crack & Npasswd**
    - **Analysis tools for verifying & enforcing compliance to policy**
    - **OTS + Scripting**

- **Intrusion Detection:**
  - **Tripwire**
    - **File system integrity checker**
    - **OTS + Scripting**

Design Description (cont.)

- **Management Proxy Agent**
  - **Provides management of the COTS**
  - **Reuse of Custom Software**

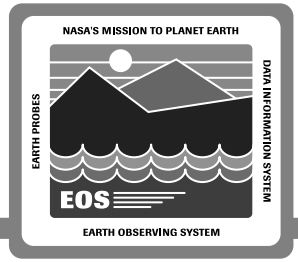
Interfaces

- **SMC**
- **External Systems**
- **Management Agent Services**

Operator Interface

- **As provided by the COTS and OTS products**

Summary



COTS (and OTS) intensive

Lowers development

Lowers maintenance costs